



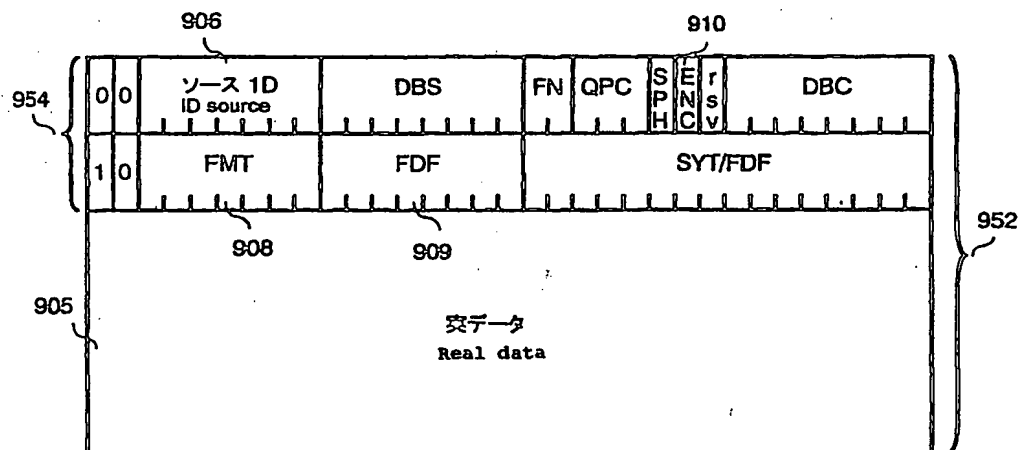
PCT

特許協力条約に基づいて公開された国際出願

<p>(51) 国際特許分類6 H04L 12/40, 9/00</p>	<p>A1</p>	<p>(11) 国際公開番号 WO98/48543</p> <p>(43) 国際公開日 1998年10月29日(29.10.98)</p>
<p>(21) 国際出願番号 PCT/JP98/01837</p> <p>(22) 国際出願日 1998年4月22日(22.04.98)</p> <p>(30) 優先権データ 特願平9/106995 1997年4月24日(24.04.97) JP</p> <p>(71) 出願人 (米国を除くすべての指定国について) 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP] 〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP)</p> <p>(72) 発明者; および</p> <p>(75) 発明者/出願人 (米国についてののみ) 西村拓也(NISHIMURA, Takuya)[JP/JP] 〒576-0021 大阪府交野市妙見坂6-1-105 Osaka, (JP) 飯塚裕之(IITSUKA, Hiroyuki)[JP/JP] 〒576-0033 大阪府交野市私市6-25-6 Osaka, (JP) 山田正純(YAMADA, Masazumi)[JP/JP] 〒570-0011 大阪府守口市金田町6-24-10 Osaka, (JP)</p> <p>(74) 代理人 弁理士 滝本智之, 外(TAKIMOTO, Tomoyuki et al.) 〒571-8501 大阪府門真市大字門真1006番地 松下電器産業株式会社内 Osaka, (JP)</p>		<p>(81) 指定国 CN, JP, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p>添付公開書類 国際調査報告書</p>

(54)Title: DATA TRANSFER METHOD

(54)発明の名称 データ転送方法



(57) Abstract

A data transfer method for preventing the malfunction of the conventional equipment which does not cope with encipherment at the time of transmitting enciphered AV information protected by a copyright through an IEEE 1394 bus. In the method, cipher identification information indicating the state of encipherment of a real data part and the real data part are contained in synchronous data transferred through isochronous communication and encipherment is effected only on the real data part. According to this method, a transmitter transmits cipher identification information indicating the state of encipherment of the real data part contained in the synchronous data together with real data and a receiver which detects the fact that the real data part has been enciphered from the cipher identification information requests the transmitter to send deciphering information and, upon receiving this information from the transmitter in response to the request, decipheres the real data part by using the deciphering information.

(57)要約

IEEE 1394バスで、著作権により保護されたAV情報を暗号化して送信する際に、暗号化に対応していない従来の機器も誤動作することのないデータ転送方法を提供することを目的とし、アイソクロノス通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行う。

同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データと一緒に送信装置から送信され、実データ部が暗号化されていることをこの暗号識別情報により検出した受信装置が、送信装置に対して復号化情報を要求し、この要求に従って送信装置から送信された復号化情報を受け取った受信装置はこの復号化情報を使用して実データ部の復号化を行うデータ転送方法。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AL	アルバニア	FI	フィンランド	LR	リベリア	SK	スロヴァキア
AM	アルメニア	FR	フランス	LS	レソト	SL	シエラ・レオネ
AT	オーストリア	GA	ガボン	LT	リトアニア	SN	セネガル
AU	オーストラリア	GB	英国	LU	ルクセンブルグ	SZ	スワジランド
AZ	アゼルバイジャン	GD	グレナダ	LV	ラトヴィア	TD	チャード
BA	ボスニア・ヘルツェゴビナ	GE	グルジア	MC	モナコ	TG	トーゴ
BB	バルバドス	GH	ガーナ	MD	モルドヴァ	TJ	タジキスタン
BE	ベルギー	GM	ガンビア	MG	マダガスカル	TM	トルクメニスタン
BF	ブルキナ・ファソ	GN	ギニア	MK	マケドニア旧ユーゴスラヴィア共和国	TR	トルコ
BG	ブルガリア	GW	ギニア・ビサウ	ML	マリ	TT	トリニダード・トバゴ
BJ	ベナン	GR	ギリシャ	MN	モンゴル	UA	ウクライナ
BR	ブラジル	HR	クロアチア	MR	モーリタニア	UG	ウガンダ
BY	ベラルーシ	HU	ハンガリー	MW	マラウイ	US	米国
CA	カナダ	ID	インドネシア	MX	メキシコ	UZ	ウズベキスタン
CF	中央アフリカ	IE	アイルランド	NE	ニジェール	VN	ヴェトナム
CG	コンゴ	IL	イスラエル	NL	オランダ	YU	ユーゴスラビア
CH	スイス	IS	アイスランド	NO	ノルウェー	ZW	ジンバブエ
CI	コートジボアール	IT	イタリア	NZ	ニュージーランド		
CM	カメルーン	JP	日本	PL	ポーランド		
CN	中国	KE	ケニア	PT	ポルトガル		
CU	キューバ	KG	キルギスタン	RO	ルーマニア		
CY	キプロス	KP	北朝鮮	RU	ロシア		
CZ	チェッコ	KR	韓国	SD	スーダン		
DE	ドイツ	KZ	カザフスタン	SE	スウェーデン		
DK	デンマーク	LC	セントルシア	SG	シンガポール		
EE	エストニア	LI	リヒテンシュタイン	SI	スロヴェニア		
ES	スペイン	LK	スリ・ランカ				

明 細 書

データ転送方法

5 技術分野

本発明は、通常のデジタルデータと暗号化されたデジタルデータとが混在するデータを転送するデジタルデータ転送方法に関するものである。

背景技術

- 10 従来のデータ転送方式には I E E E 1 3 9 4 規格 (IEEE: THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.) を用いたデータ転送方法がある (参考文献: IEEE Std 1394:1995, High Performance Serial Bus)。
- I E E E 1 3 9 4 規格におけるデータ転送には、デジタル映像信号やデジタル音声信号等の同期データの転送に適したアイソクロノス (isochronous) 通信と、制御信号等の非同期データの伝送に適したエイシンクロナス (asynchronous) 通信とがあり、両方の通信は I E E E 1 3 9 4 バス上で使用することが可能である。アイソクロノス通信はいわゆる放送型の通信であり、I E E E 1 3 9 4 バス上の 1 つの装置が出力するアイソクロノス packets を、同バス上の全ての装置が受信することができる。これに対してエイシンクロナス通信
- 15 には 1 対 1 の通信と 1 対 N の放送型通信の両方があり、バス上の 1 つの装置が出力するエイシンクロナス packets には、その packets を受信すべき装置をあらわす識別子が含まれており、その識別子が特定の装置をあらわす時にはその識別子で指定された装置が当該エイシンクロナス packets を受信し、その識別子がブロードキャストをあらわす時には同バス上の全ての装置が当該エイシンクロナス packets を受信する。
- 20 25

また、IEEE 1394規格に準拠したデータ転送方法を用いて、デジタル音声信号やデジタル映像信号等を転送したり、IEEE 1394バス上に接続された機器間でのデータ伝送を行うための規格として、IEC (IEC: International Electrotechnical Commission 国際電気標準会議) においてIEC 1883規格 (以下、AVプロトコルと称する) が検討されている。AVプロトコルにおいては、映像音声データは図5に示すアイソクロノスケット内に配置されて転送される。また、アイソクロノスケットはCIPヘッダ (CIP: Common Isochronous Packet) を含む。CIPヘッダ内には、映像音声データの種別を示す識別情報やアイソクロノスケットを送信している送信装置の装置番号等の情報が含まれている。

図5はAVプロトコルにて使用されるアイソクロノスケットのフォーマットをあらわす図である。アイソクロノスケットは、アイソクロノスケットヘッダ900、ヘッダCRC901、アイソクロノスペイロード902およびデータCRC903からなる。アイソクロノスケットヘッダ900にはタグ907が含まれる。タグ907は、その値が1である時には、そのアイソクロノスケットがAVプロトコルに準拠していることを示す。タグ907の値が1であるとき、すなわちそのアイソクロノスケットがAVプロトコル準拠のアイソクロノスケットである時には、アイソクロノスペイロード902の先頭にCIPヘッダ904が含まれる。CIPヘッダ904の中には、当該アイソクロノスケットを出力している出力装置の識別子であるソースID906が含まれる。また、CIPヘッダ904には、アイソクロノスペイロード902に含まれる実データ905がどのような種類のデータであるかをあらわすFMT908とFDF909が含まれる。映像信号や音声信号のデジタルデータは実データ905に含まれるが、実データ905はアイソクロノスペイロード902にかならず含まれるとは限らず、ケットによっては実データ905を含まずにCIPヘッダ904のみを含

むアイソクロノスペイロード 9 0 2 も有り得る。

また、AV プロトコル上で機器制御を行うためのコマンド群として、AV/C コマンドセットがある。(参考文献: 1394 TRADE ASSOCIATION Specification for AV/C Digital Interface Command Set Version 1.0

5 September 13, 1996) これらのコマンドとその応答はエイシンクロナス通信を用いて転送される。

前記従来のデータ転送方法において、著作権保護のためにアイソクロノスペイロード 9 0 2 を暗号化したアイソクロノスパケットをアイソクロノス通信で送信しようとする、暗号化されたアイソクロノスペイロード 9 0 2 の転送に対応し
10 ていない従来の機器との互換性が保たれなくなる。すなわち、従来の機器は、アイソクロノスペイロード 9 0 2 の先頭に C I P ヘッダ 9 0 4 が正常に配置されて送信されてくることを前提に作られているので、アイソクロノスペイロード 9 0 2 が暗号化されていると、従来の機器では C I P ヘッダ 9 0 4 が正常に読み出されず、そのアイソクロノスパケットは AV プロトコルを満たさないものと判断さ
15 れ、暗号化されたアイソクロノスパケットを受信した受信装置は正常に動作することができなくなる。すなわちその受信装置では実データ 9 0 5 に含まれるデータがどのような種類のデータであるかを判別することが不可能であり、当該アイソクロノスパケットを出力している装置を特定することが不可能になるので、かつ当該送信装置に対する各種の問い合わせ等のエイシンクロナス通信を行うこと
20 ができなくなり、受信動作を正常に行うことが不可能になってしまうという課題があった。

また前記従来のデータ転送方法において、送信装置が出力するアイソクロノスパケットを、受信装置が継続して受信している最中にアイソクロノスパケットの暗号化が始るような場合、従来の機器においては、暗号化が始まった途端に C I
25 P ヘッダ 9 0 4 を正常に読み出すことができなくなり、正常な受信が行えなくな

るという課題があった。

また送信装置が、著作権で保護されている映像音声情報等を暗号化して送信し、正規に認められた受信装置が、その暗号化された映像音声データ等を復号化するためには、送信装置は、正規の受信装置に対して復号のための復号化情報を付与
5 する必要がある。その場合、前記従来のデータ転送方法においては、送信装置が受信装置を特定するには非常に煩雑な手順を実行せねばならない。すなわちアイソクロノスケットには、送信を行っている装置の識別子であるソースID906は含まれるが、どの装置が当該アイソクロノスケットを受信するべきかをあ
10 らわす情報は含まれておらず、そのため送信装置はどの装置が当該アイソクロノスケットの受信を行っているかをアイソクロノスケット送信中に調べることはできない。そこで、送信装置が、IEEE1394バス上に接続されている機器のうちのどの機器が受信を行っているかを調べるには、送信装置はバス上の全ての機器に対して受信状態の問い合わせを順次に行わねばならず、復号のための鍵情報を付与する手順が非常に煩雑になるという課題があった。

15 本発明は、前記従来の問題点を解決するもので、暗号化した映像音声情報をアイソクロノス通信で送信する場合にも従来の通信規格を満足し、かつ従来の受信装置が暗号化された映像音声データを含むアイソクロノスケットを受信しても誤動作することのないデータ転送方法を実現することを目的とする。

また本発明は、前記従来の問題点を解決するもので、送信装置が正規の受信装
20 置に復号のための鍵情報を付与する手順を極めて簡素なものにすることが可能なデータ転送方法を実現することを目的とする。

発明の開示

前記従来のデータ転送方法の問題点を解決するために、本発明のデータ転送方
25 法においては、アイソクロノス通信で転送される同期データには実データ部の暗

号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行う。

また前記従来のデータ転送方法の問題点を解決するために、本発明のデータ転送方法においては、同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データと一緒に送信装置から送信され、実データ部が暗号化されていることをこの暗号識別情報により検出した受信装置が、送信装置に対して復号化情報を要求し、この要求に従って送信装置から送信された復号化情報を受け取った受信装置はこの復号化情報を使用して実データ部の復号化を行うことによってデータ転送が行われる。

- 10 本発明のデータ転送方法においては、同期データを受信した受信装置が、同期データ内に含まれる暗号識別情報を調べ、実データ部が暗号化されていることを検出すると、送信装置に対して実データ部を復号するための復号化情報を要求する。この要求はA V / Cセット中のコマンドによりエイシンクロナス通信を用いて行われ、この要求を受け取った送信装置においては、受け取ったコマンドのパ
- 15 ケットヘッダを調べることにより、要求を出した機器すなわち受信装置が特定される。ここで特定された受信装置に対して送信装置が復号化情報をエイシンクロナス通信によりコマンドで付与することにより、送信装置が受信装置に復号のための復号化情報を付与する手順が極めて簡素なデータ転送方法を実現できる。

- また本発明のデータ転送方法においては、同期データの暗号化は実データ部のみに対して行われ、同期データには実データ部の暗号化状況を示す暗号識別情報が含まれる。これにより、C I Pヘッダは暗号化されずにそのまま転送されるので、従来の装置がこれらの暗号化された同期データを受信しても誤動作することはない。すなわち、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が暗号化された同期データを受信しても誤動作する可能性の無いデータ転
- 20
- 25 送方法を実現できる。

また本発明のデータ転送においては、送信装置の送信している同期データを受信装置が継続的に受信している最中に、同期データの暗号化が始まったとしても、C I Pヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できる。

5

図面の簡単な説明

図 1 は本発明の実施形態におけるC I Pヘッダのフォーマットを表す模式図、

図 2 は本発明の実施形態における送信装置と受信装置との機能を表すブロック図、

10 図 3 A は本発明の実施形態におけるAKEステータスコマンドのフォーマットを表す図、

図 3 B は本発明の実施形態におけるAKEステータスコマンドに対するAKEレスポンスのフォーマットを表す図

15 図 3 C は本発明の実施形態におけるAKEコントロールコマンドのフォーマットを表す図

図 4 は本発明の実施形態における送信装置と受信装置との間で伝送されるエイシンクロナスパケットの伝送手順を表す模式図、

図 5 は従来のデータ転送方法におけるアイソクロノスパケットのフォーマットを表す図。

20

発明を実施するための最良の形態

以下、本発明の第一の実施形態について、図面を参照しながら説明する。

図 1 は本発明の実施形態において転送されるアイソクロノスパケットのペイロード部の形式を表した図である。本実施形態はM P E G (Moving Picture Expert Group)に準拠したT S P (トランスポートパケット) の転送例である。

25

ENC（以下暗号化情報と記す） 9 1 0は実データ 9 0 5が暗号化されているか否かを示す。

図 2 は本発明の実施形態における送信装置と受信装置の関係をあらわす図である。送信装置 1 1 0 と受信装置 1 2 8 とは IEEE 1 3 9 4 バス（以下 1 3 9 4
5 バスと記す） 1 1 1 を通じてつながれている。

先ず送信装置 1 1 0 における各ブロックの機能を以下に説明する。

信号源 1 0 0 は、1 3 9 4 バス 1 1 1 上に送信しようとする 1 8 8 バイト単位の MPEG のトランスポートパケット TSP（図示せず）を暗号化手段 1 0 1 に対して出力する。すなわち本実施形態では、信号源 1 0 0 は 1 8 8 バイトの固定
10 長のデータを出力する。暗号化手段 1 0 1 は鍵生成手段 1 0 6 から与えられる暗号鍵 1 0 9 を用いて信号源 1 0 0 から受け取った TSP を暗号化して出力する。本実施形態では暗号化鍵 1 0 9 が復号化情報に相当する。出力命令 1 0 5 は鍵生成手段 1 0 6 から暗号化手段 1 0 1 に対する命令であり、通常出力、暗号化出力および空出力の 3 種類の命令がある。出力命令 1 0 5 を受け取った暗号化手段 1
15 0 1 は、その命令の内容が通常出力である場合には、信号源 1 0 0 から受け取った TSP をそのまま出力し、暗号化情報 9 1 0 には値 0 を出力する。また出力命令 1 0 5 の内容が暗号化出力である場合には、TSP を鍵生成手段 1 0 6 から受け取った暗号鍵 1 0 9 で暗号化して出力し、暗号化情報 9 1 0 には値 1 を出力する。また出力命令 1 0 5 の内容が空出力である場合には、信号源 1 0 0 から TS
20 P を受け取るたびに空信号（図示せず）を出力するとともに、暗号化情報 9 1 0 には値 1 を出力する。ソースパケット化手段 1 0 2 は、暗号化手段 1 0 1 から受け取った 1 8 8 バイトの TSP に 4 バイトのソースパケットヘッダを付加して 1 9 2 バイトのソースパケット（実データ 9 0 5）を出力する。CIP ブロック化手段 1 0 3 は、ソースパケット化手段 1 0 2 から受け取ったソースパケットに C
25 IP ヘッダ 9 5 4 を付加してアイソクロノスペイロード 9 5 2 を出力する。その

際にCIPブロック化手段103は、暗号化手段101から受け取った暗号化情報910をCIPヘッダ954内に配置する。アイソクロノスパケット化手段107はCIPブロック化手段103から受け取ったアイソクロノスペイロード952にアイソクロノスパケットヘッダ900、ヘッダCRC901およびデータCRC903を付加してアイソクロノスパケットを出力する。このとき、アイソクロノスペイロード952の内容がAVプロトコルに準拠したデータであるので、タグ907の値は1とする。鍵生成手段106は、後述するように受信装置128との間で、図3に示すエイシンクロナスパケットのやりとりにより暗号鍵109を受信装置128に送信し、また前述のように暗号化手段101に対しても暗号鍵109を出力する。

1394パケット入出力手段108は、1394バス111と送信装置110との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、1394パケット入出力手段108は、アイソクロノスパケット化手段107から受け取ったアイソクロノスパケットおよび鍵生成手段106から受け取ったエイシンクロナスパケットを1394バス111上に出力するとともに、1394バス111から受信したエイシンクロナスパケットを鍵生成手段106へと出力する。

次に受信装置128の各ブロックの機能を以下に説明する。

1394パケット入出力手段127は、1394バス111と受信装置128との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、1394パケット入出力手段127は、1394バス111から受信したアイソクロノスパケットをペイロード抽出手段123に対して出力し、1394バス111から受信したエイシンクロナスパケットを鍵生成手段125に対して出力する。また、鍵生成手段125から受け取ったエイシンクロナスパケットを1394バス111に対して出力する。

ペイロード抽出手段123は、1394バス111から受信したアイソクロノ
スパケットを1394パケット入出力手段127から受取り、アイソクロノスパ
ケットのタグ907の値が1である場合にはアイソクロノスペイロード952の
中身がAVプロトコル準拠のデータであることを知り、アイソクロノスペイロー
ド952を実データ抽出手段122に対して出力する。実データ抽出手段122
は、受けとったアイソクロノスペイロード952に実データ905が含まれる場
合には、アイソクロノスペイロード952の先頭のCIPヘッダ954を除去し
た実データ905を復号化手段121に対して出力する。また、実データ抽出手
段122は、CIPヘッダ954から抽出したソースID906と暗号化情
報910とを鍵生成手段125に対して出力する。また暗号化情報910は、復
号化手段121に対しても同様に出力される。鍵生成手段125は、後述するよ
うに送信装置110との間でのエイシンクロナス通信によるエイシンクロナスパ
ケットのやりとりにより暗号鍵126を受け取り、復号化手段121に対して暗
号鍵126を出力する。復号化手段121は、実データ抽出手段122から受信
した暗号化情報910の値が0の時には、実データ抽出手段122から受け取っ
た実データ905を映像音声化手段120に対してそのまま出力し、暗号化情報
910の値が1の時には、鍵生成手段125から受け取った暗号鍵126を用い
て実データ905を復号化し、復号化した結果を映像音声化手段120に対して
出力する。

次に前述のエイシンクロナス通信によるエイシンクロナスパケット伝送につい
て説明する。

図3A～Cは、エイシンクロナス通信により伝送されるエイシンクロナスパケ
ットのフォーマットを示し、このうち図3Aおよび図3Cは、本実施形態におけ
る鍵生成手段106と鍵生成手段125との間でやりとりされるAKEコマンド

(AKE: Authentication and Key Exchange)のコマンドフォーマットであ

り、図3Bはレスポンスフォーマットである。これらのコマンドおよびレスポンスは、AV/Cコマンドセットに属するコマンドとして、エイシンクロナス通信を用いて送信装置110と受信装置128との間でやり取りされる。これらのコマンドおよびレスポンスをやりとりすることにより、送信装置110および受信装置128の間で、相手装置の認証や暗号鍵109、126のやりとりに必要な情報の交換が行われる。前記AKEコマンドには、相手装置に対する何らかの動作を要求するAKEコントロールコマンドと、相手装置の状態や能力を問い合わせるためのAKEステータスコマンドとがある。

図3AはAKEステータスコマンドのフォーマットをあらわす図である。AKEステータスコマンドにおいて、オペコード208は、当該コマンドがAKEコマンドであることを示す。アルゴリズムID200は固定値0であり、0以外の値は将来の拡張のために予約となっている。

図3BはAKEステータスコマンドに対するレスポンスのフォーマットをあらわす。図3AのAKEステータスコマンドを受け取った装置が、そのAKEステータスコマンドを発行した装置に対して返送するのがこのレスポンスである。送信装置110と受信装置128との間で、相互認証および暗号鍵109、126の伝達を行う一連の情報交換手順には複数の種類があり、アルゴリズム領域201には、当該レスポンスを返す装置が実行可能な情報交換手順の識別子がビットアサインされている。すなわち、受信装置128は、前記の手順により暗号化されたTSPを検出してから暗号鍵109、126を受け取るまでの間に、送信装置110との間で複数のコマンドおよびレスポンスをやり取りする。このコマンドおよびレスポンスをやり取りする情報交換手順には複数の種類があり、当該レスポンスを返す装置は、自身で実行可能な情報交換手順をアルゴリズム領域201における当該ビットの値を1にしてあらわす。アルゴリズム領域201のサイズは16ビットであるので、最大16種類の情報交換手順をあらわすことが可能

である。最大データ長 2 1 2 は、AKE コマンドおよびそれに対するレスポンス
をやり取りする際に、受信可能な最大データ長が何バイトであることを示す。

図 3 C は AKE コントロールコマンドのフォーマットをあらわす。AKE コン
トロールコマンドにおけるアルゴリズム領域 2 0 1 は、アルゴリズム ID 2 0 0
5 の値が 0 である時には、実行中の情報交換手順をあらわす。アルゴリズム領域 2
0 1 の各ビットは、AKE コントロールコマンドおよび AKE コントロールコマ
ンドに対するレスポンスにおいては、必ず 1 つのビットだけが 1 で他のビットは
0 となっており、その値 1 の 1 ビットが現在実行中の情報交換手順をあらわして
いる。ラベル 2 0 2 は、複数の AKE コントロールコマンド間の対応を明確にし
10 るために用いられる。例えば、1 つの装置が他の装置に対して AKE コントロー
ルコマンドを送信したとして、その AKE コントロールコマンドを受信した装置
は、受信した AKE コントロールコマンドに呼応する別の AKE コントロールコ
マンド返送するという規定が、ある情報交換手順で定められているとする。この
場合、両 AKE コントロールコマンド間の呼応関係を明確にするために、返送す
15 る AKE コントロールコマンドに挿入されるラベル 2 0 2 は、最初に受信した A
KE コントロールコマンドに挿入されていたラベル 2 0 2 と同じ値を使用する。
ステップ番号 2 0 3 は、情報交換手順の中でやりとりされる順に、個々の AKE
コントロールコマンドに対して 1 から順に付けられるシリアル番号である。

サブファンクション 2 9 9 は、表 1 に示す値をとり、この値によってその AK
20 E コマンドの持つ意味が定まる。

表 1

サブファンクション	値
メイクレスポンス	00 ₁₆
ベリファイミー	01 ₁₆
クリエイトキーインフォ	10 ₁₆
リコンストラクトキー	11 ₁₆
エクスチェンジ	20 ₁₆

サブファンクション299の内容がメイクレスポンスである場合には、当該AKEコントロールコマンドはコマンドを受信する装置に対する認証のチャレンジを意味する。このときデータ207には、相手の装置を認証するための乱数である認証チャレンジデータが含まれる。このコマンドを受信した装置は、サブファンクション299の内容をベリファイミにしたAKEコントロールコマンドを返送する。この返送の際にデータ207に格納されるデータは、先程受信したデータ207中の認証チャレンジデータに対して、あらかじめ定められた演算を行った結果である認証レスポンスデータである。この演算に使用される鍵情報は、あらかじめ正規に認定された機器にのみ付与されている鍵であるので、返送されてきた認証レスポンスデータを調べれば、演算を行った機器が正しく認定された機器であるか否かを認証することができる。

サブファンクション299の内容がクリエイトキーインフォである場合には、当該AKEコントロールコマンドは、このコマンドを受信する装置に対する暗号鍵109の要求を意味する。このAKEコントロールコマンドを受け取った装置は、サブファンクション299の内容がリコンストラクトキーであるAKEコントロールコマンドを返送する。この時、データ207には暗号化された暗号鍵109が格納されて返送される。

サブファンクション299の内容がエクスチェンジである場合には、当該AKEコントロールコマンドは、コマンドを送信する機器と受信する機器との間での鍵情報の交換を意味する。この鍵情報はデータ207に格納されて転送され、機器間の間接認証や、機器共有鍵の作成のために使用される。

表1に挙げられている以外のサブファンクションの値は将来における拡張のための予約となっている。チャンネル番号204は、送信装置110と受信装置128との間で行うアイソクロノス通信のチャンネルの番号を示す。このチャンネル番号

204は、サブファンクション299の内容がクリエイトキーインフォまたはリ
コンストラクトキーの時にのみ有効であり、それ以外の場合にはこの値は16進
表記でFFとなる。ブロック番号205および総ブロック番号206は、AKE
コントロールコマンドでやり取りすべきデータが一つのAKEコマンドで伝送し
5 きれない場合に使用する。すなわちこの場合には、当該データはいくつかのプロ
ックに分割され、複数回に分けて転送される。総ブロック番号206は当該デー
タを分割したブロック個数をあらわし、ブロック番号205は、データ207が
幾つ目のブロックのデータであるかを示す。データ長209はデータ207に含
まれる有効なデータ長をバイト数で表す。データ207はAKEコントロールコ
10 マンドによってやり取りされるデータである。AKEコントロールコマンドを受
信した装置はそのAKEコントロールコマンドに対する応答を返す。その際の応
答のフォーマットおよび値は、受け取ったAKEコントロールコマンドのフォー
マットおよび値と同じであるが、応答にはデータ207が含まれない点だけが唯
一異なる。

15 図4は、送信装置110から受信装置128に対して暗号鍵109、126が
送信されるまでの間に、両装置間でやり取りされるAV/Cコマンドの具体例を
時系列で模式的にあらわした図である。まず、図4に示すAV/Cコマンドのや
り取りが始まるまでの両装置の動作を簡単に説明する。

まず初期状態として、暗号化されていないTSPが送信装置110から送信さ
20 れている状況を想定する。信号源100から出力されるTSPが暗号化手段10
1に入力される。暗号化手段101は、出力命令105の内容が通常出力である
ので、TSPを暗号化せずにそのままソースパケット化手段102へ出力すると
ともに、暗号化情報910には値0を出力する。ソースパケット化手段102は、
受け取ったTSPに4バイトのソースパケットヘッダを付加して、CIPブロッ
25 ク化手段103へ出力する。CIPブロック手段103は、これに8バイトのC

IPヘッダ954を付加し、アイソクロノスケット化手段107に対して、アイソクロノスペイロード952として出力する。この際、CIPヘッダ954に含まれる暗号化情報910には、暗号化手段101から入力した値である0をそのまま格納する。アイソクロノスケット化手段107は、受け取ったアイソクロノスペイロード952に、アイソクロノスケットヘッダ900、ヘッダCRC901およびデータCRC903を付加して、アイソクロノスケットを作成する。このアイソクロノスケットは、1394パケット入出力手段108によって1394バス111上へ出力される。この際、当該アイソクロノスケットがAVプロトコル準拠のアイソクロノスケットであるので、アイソクロノスケットヘッダ900に含まれるタグ907の値は1となる。

信号源100から出力されるTSPが変化した時、すなわち著作権で保護されていない映像音声情報から著作権で保護されている映像音声情報へと切り替わった時、この変化を検出した鍵生成手段106は、出力命令105を通常出力から空出力へと変化させるとともに、TSPを暗号化するための暗号鍵109を暗号化手段101に渡す。

出力命令105の内容が空出力であるとき、暗号化手段101は、信号源100からTSPを受け取るたびにソースパケット化手段102に対して空信号を出力するとともに暗号化情報910に値1を出力する。暗号化手段101から空信号を受け取ったソースパケット化手段102は、ソースパケットヘッダを付加せずに、受け取った空信号をそのままCIPブロック化手段103へと伝達する。CIPブロック化手段103は空信号を受け取ると、CIPヘッダ954だけをアイソクロノスケット化手段107へ出力する。この時、CIPヘッダ954中の暗号化情報910は、暗号化手段101が出力した値1をそのまま用いる。アイソクロノスケット化手段107は、CIPブロック化手段103から受け取ったCIPヘッダ954をアイソクロノスペイロード952としてアイソクロ

ノスパケットを作成し、1394パケット入出力手段108へ出力する。この際、当該アイソクロノスパケットはAVプロトコルに準拠しているので、タグ907の値は1となる。1394パケット入出力手段108は受け取ったアイソクロノスパケットを1394バス111上へ出力する。当該アイソクロノスパケットは

5 継続的に出力され、1394バス111上にはCIPヘッダ954のみをアイソクロノスペイロード952に含んだアイソクロノスパケットが継続的に流れるようになる。このアイソクロノスパケットを受信した受信装置128では、1394パケット入出力手段127がタグ907を調べ、AVプロトコルに準拠したアイソクロノスパケットであることを検出した後、当該アイソクロノスパケットを

10 ペイロード抽出手段123へ出力する。ペイロード抽出手段123は受け取ったアイソクロノスパケットからアイソクロノスペイロード952を抽出して実データ抽出手段122へ出力する。実データ抽出手段122は、CIPヘッダ954に含まれる暗号化情報910とソースID906とを鍵生成手段125へ出力する。鍵生成手段125は、暗号化情報910を調べて値が1であることを検出したのち、ソースID906から当該アイソクロノスパケットを出力しているのが

15 出力装置110であることを知る。しかる後、鍵生成手段125はAV/Cコマンドを用いて暗号鍵109、126を要求する過程、すなわち図4に示した過程へと移る。

図4において、先ずAKEステータスコマンド300が受信装置128から送信装置110へ送信される。これにより受信装置128は、送信装置110が実行可能な情報交換手順を問い合わせることになる。これに応じて送信装置110はAKEレスポンス301を受信装置128に対して返送する。このAKEレスポンス301には、送信装置110が実行可能な情報交換手順が、アルゴリズム領域201内にビットアサインされており、これによって受信装置128は、送信装置110がどの情報交換手順を実行可能なのかを知ることができる。具体例

20

25

としては、送信装置 110 が実行可能な情報交換手順が第 2 番目のものと第 6 番目のものの 2 つであった場合には、AKE レスポンス 301 内のアルゴリズム領域 201 は 2 進表記で 0000000000100010 となる。

5 AKE レスポンス 301 を受信した受信装置 128 は、送信装置 110 が実行可能でかつ受信装置 128 自身も実行可能な情報交換手順の中から、最適な 1 つの手順を選択し、以降その手順にしたがって AV/C コマンドをやりとりする。いま仮に受信装置 128 の側で、実行可能な情報交換手順が第 2 番目のものと第 8 番目のものであった場合には、送信装置 110 および受信装置 128 の双方で
10 実行可能な情報交換手順は、第 2 番目のものだけということになり、以降は第 2 番目の手順を用いて認証および情報の交換が行われることになる。この手順に含まれる AKE コントロールコマンドでは、アルゴリズム ID の値が 0 で、アルゴリズム領域 201 の値が 16 進表記で 0000000000000010 となる。情報交換手順で指定される手順には、各種 AKE コントロールコマンドのやり取りの順番だけでなく、各 AKE コントロールコマンドで送られるデータ 207 のフォーマットや処理方法も規定されている。
15

第 2 番目の情報交換手順に従い、鍵生成手段 125 はメイクレスポンスコマンド 302 を送信装置 110 に対して送信する。このメイクレスポンスコマンド 302 中のデータ 207 には、鍵生成手段 125 で発生させた 2 つの乱数、RRa と RRb とが暗号化されて含まれているとともに、アルゴリズム領域 201 には第 2 番目の手順をあらわす識別情報が含まれている。この暗号化に際して使用する鍵は、正規に認められた送信装置と受信装置とにあらかじめ与えられている
20 共通の秘密鍵である。メイクレスポンスコマンド 302 を受け取った鍵生成手段 106 は、受け取ったメイクレスポンスコマンド 302 のアルゴリズム領域 201 を調べて、以降は第 2 番目の手順を用いて認証および情報の交換を行うことを
25 知る。鍵生成手段 106 は、第 2 番目の手順を実行可能なのであるから、第 2 番

目の手順に基づいて送信されてくるメイクレスポンスコマンド302のデータ207にはこの秘密鍵で暗号化された2つの乱数が含まれていることを知っている。そこで鍵生成手段106は、この秘密鍵を用いてデータ207からRRaおよびRRbの2つの乱数を取り出したのち、レスポンスを作成することが可能であることを示す応答303を返す。しかるのち鍵生成手段106は、取り出した乱数のうちの一つであるRRaをデータ207に格納して、ベリファイミーコマンド304を受信装置128に対して送信する。これが先程のメイクレスポンスコマンド302にて要求されたレスポンスである。このベリファイミーコマンド304を含め、これ以降、送信装置110と受信装置128との間でやり取りされる各AKEコマンドのアルゴリズム領域201には全て、2番目の手順をあらわす識別情報が含まれる。

ベリファイミーコマンド304を受信した鍵生成手段125は、データ207の内容であるRRaが、自分が先程発生させた乱数RRaと一致することを確認したのち、ベリファイミーコマンド304に対して、正常にベリファイしたことを示す応答305を返す。これにより、鍵生成手段125は、送信装置110が正規に認められた送信装置であると認証する。

次に送信装置110は、前記メイクレスポンス302以降と同じ手順によって、メイクレスポンスコマンド306およびベリファイミーコマンド308を用いて、受信装置128が正規に認められた受信装置であることを確認する。但しこの際に使用される乱数はRTaおよびRTbであり、ベリファイミーコマンド308で送り返される乱数はRTbである。

この時点で送信装置110および受信装置128の双方は、乱数RRbと乱数RTbとがともにわかっていることになり、また、お互いが正規に認められた装置であることを確認したことになる。鍵生成手段106と鍵生成手段125とは、それぞれ別個に、2番目の手順で定められている共通の演算方法により、RRb

とRTbとから一時鍵（図示せず）を生成する。この一時鍵は、送信装置110および受信装置128の両装置のみが共有する共通の鍵である。

次に鍵生成手段125はクリエイトキーインフォコマン
5 ド310を送信装置110に対して送信する。この際、クリエイトキーインフォコマン
ド310のチャネル番号204には、現在受信装置128が受信中のアイソクロノスパケットの
チャネル番号が格納される。このクリエイトキーインフォコマン
ド310を受け取った鍵生成手段106は、TSPの暗号化に用いる暗号鍵109を前記の一時
10 鍵で暗号化したのち、クリエイトキーインフォコマン
ド310が正常に完了したことを示す応答311を返送する。続いて、鍵生成手段106は、この暗号鍵1
09を一時鍵で暗号化した結果をデータ207に格納したりリコンストラクトキー
コマン
ド312を受信装置128へ送る。鍵生成手段125は一時鍵を用いて、
受け取ったリコンストラクトキーコマン
ド312のデータ207を復号化し、その結果暗号鍵126を得たのち、リコンストラクトキーコマン
ド312を正常に完了したことをあらわす応答313を返す。暗号鍵109と暗号鍵126とは、
15 同じ一時鍵を用いて暗号化と復号化を行ったので、同じ鍵である。この暗号鍵1
26は鍵生成手段125から復号化手段121に対して出力される。以上の手順
で復号化情報の付与が完了する。

リコンストラクトキーコマン
ド312を送信した鍵生成手段106は、暗号化
手段101に対して暗号化出力を示す出力命令105を出力する。これを受けた
20 暗号化手段101は、信号源100から受け取るTSPを暗号鍵109で暗号化
し、ソースパケット化手段102への出力を開始する。これにより、1394バ
ス111上に、暗号鍵109にて暗号化されたTSPをアイソクロノスペイロー
ド952に含むアイソクロノスパケットが送信装置110から送信されるよう
になる。受信装置128で受信された当該アイソクロノスパケットは、前述したよ
25 うに、復号化手段121において暗号鍵126を用いて復号化され、映像音声化

手段 1 2 0 へ出力される。

前記一連のAKEコントロールコマンドにおいて、メイクレスポンスコマンド 3 0 2 とベリファイミーコマンド 3 0 4、メイクレスポンスコマンド 3 0 6 とベリファイミーコマンド 3 0 8、およびクリエイトキーインフォコマンド 3 1 0 と
5 リコンストラクトキーコマンド 3 1 2 はそれぞれ同じラベル 2 0 2 を持つ。また、メイクレスポンスコマンド 3 0 2、ベリファイミーコマンド 3 0 4、メイクレスポンスコマンド 3 0 6、ベリファイミーコマンド 3 0 8、クリエイトキーインフォコマンド 3 1 0 およびリコンストラクトキーコマンド 3 1 2 はそれぞれ 1、2、3、4、5、6 なる値をステップ番号 2 0 3 に持つ。

10 送信装置 1 1 0 の出力するアイソクロノスケットに含まれる実データ部 1 0 5 が、暗号化された実データ 1 0 5 から暗号化されない実データ 1 0 5 へと変化した場合には、復号化手段 1 2 1 は、暗号化情報 9 1 0 の変化を検出して復号化をやめ、実データ抽出手段 1 2 2 から受け取った出力をそのまま映像音声化手段 1 2 0 へと渡すようになる。

15 また、前記の図 4 に示した過程が始まった後に、1 3 9 4 バス 1 1 1 にバスリセットが発生した場合には、メイクレスポンスコマンド 3 0 2 以降の手順を最初からやりなおす。

以上のように本実施形態によれば、アイソクロノスケット内の実データの暗号化状況を示す暗号化情報が実データと一緒に送信装置から送信されることにより、アイソクロノスケットを受信した受信装置は、アイソクロノスケット内
20 に含まれる暗号化情報を調べ、実データが暗号化されていることを検出すると、送信装置に対して実データを復号するための暗号鍵を要求し、要求を受けた送信装置はその受信装置に対して暗号鍵を付与するので、送信装置が受信装置に復号のための暗号鍵を付与する際の手順が極めて簡素なデータ転送方法を実現できる。

25 また以上のように本実施形態によれば、アイソクロノス通信で転送されるアイ

ソクロノスパケットには、実データの暗号化状況を示す暗号化情報と実データとが含まれ、暗号化は実データに対してのみ行ってデータ転送を行うことにより、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が、暗号化された実データを受信しても誤動作する可能性のないデータ転送方法を実現できる。

- 5 また以上のように本実施形態によれば、送信装置の送信している同期データを受信装置が継続的に受信している最中に、同期データの暗号化が始まったとしても、C I Pヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できる。

- 10 なお、本実施形態においては、暗号鍵による暗号化が一旦開始されれば、全ての転送単位に含まれる実データは暗号化されて送信されるが、全ての転送単位に対して暗号化を行う必要はない。例えば暗号化された転送単位と暗号化されない転送単位とが交互に送信されても、C I Pヘッダ中に暗号化情報が含まれているので、受信装置においては復号を正常に行うことが可能であり、同様の効果を得ることが可能である。更にこの場合、暗号化を行う転送単位の割合を受信装置が
- 15 送信装置に指定しても、得られる効果が変わらないことは言うまでもない。但し、M P E Gのソースパケットはその大きさが192バイトであるが、M E P Gの高データレート転送（12Mbps以上）を行う際には複数のソースパケットが一つのアイソクロノスペイロードに格納される。このとき、同一のアイソクロノスペイロードの中に、暗号化されたソースパケットと暗号化されないソースパケッ
- 20 トとの両方があってはならないことも言うまでもない。

- 25 なお、本実施形態においては、暗号鍵による暗号化は実データ部全てに対して行われたが、全ての部分に暗号化を行う必要はない。例えば、実データ部の前半分だけを暗号化したり、実データ部を4等分したうちの最初と3番目の2個所を暗号化して送信しても同様の効果が得られる。この場合は、暗号化を行った場所
- や割合を示す情報をC I Pヘッダに挿入して送信すれば、受信装置側で適切な復

号化を行うことが可能である。更に、C I P ヘッダには、実データが暗号化されているか否かを示す暗号化情報のみを挿入しておき、C I P ヘッダを見て暗号化されていることを検出した受信装置が、実データ部のどの部分がどのくらい暗号化されているかという情報を、エイシンクロナス通信によって送信装置に問い合わせ

5 わせても、同様の効果を得ることが可能である。この場合、暗号化を行う場所や割合を、受信装置が送信装置に対してエイシンクロナス通信を用いて指定しても、同様の効果が得られることは言うまでもない。また、実データ部の中でデータの重要性が高い部分についてのみ暗号化を行うと、暗号化および復号化にかかる負荷が低くなり、しかも十分な暗号化の効果が得られることも言うまでもない。

10 なお、本実施形態においては、送信装置と受信装置との間で相互の認証が完了するまでは実データを含まないC I P ヘッダのみのアイソクロノスケットを転送したが、C I P ヘッダのみのアイソクロノスケットを出力することなく、最初から暗号化された実データを含むアイソクロノスケットを出力しても、同様の効果が得られることは言うまでもない。

15 なお、本実施形態においては、送信装置と受信装置の間でやりとりされるAKEコントロールコマンドの転送手順を相互の調停により決定したが、受信装置が実行可能な手順が一つだけに限られる場合にはこの調停手順をおこなわず、受信装置が実行可能な唯一の手順でコマンドの転送を開始しても同様の効果が得られることは言うまでもない。この場合には、全ての正規に認証された機器が最低限

20 実行可能な基本手順を定めておくことが望ましい。

なお、本実施形態においては、送信装置と受信装置との間で直接認証を行い、秘密鍵による復号化情報の伝送を行ったが、認証および復号化情報の伝達手段はこれに限らない。例えば公開鍵を用いて相互に間接認証および一時鍵の作成を行ない、一時鍵を用いて復号化情報の伝送を行っても構わない。以下、その手順を

25 簡単に説明する。

送信装置および受信装置は、相互の調停で定めた手順により、相互の間接認証に必要となる鍵情報をAKEコントロールコマンドのデータ207に格納して送信しあう。このとき、サブファンクション299はエクスチェンジをあらわす。これにより、送信装置と受信装置は、互いに正規に認証された機器であれば同じ一時鍵を共有することになるので、それ以降は本実施形態と同様の手順で、ク
5 リートキーインフォコマンドおよびリコンストラクトキーコマンドを用いて復号化情報の伝送を行うことが可能となる。

なお、本実施形態においては、送信装置と受信装置の間でやりとりされるAKE
Eコントロールコマンドの転送手順は相互の調停により決定されたが、送信装置
10 で実行可能な手順の種類があらかじめわかっている場合には、この調停手順をおこなわずに、送信装置の実行可能な手順で受信装置がコマンドの転送を開始しても、同様の効果が得られることは言うまでもない。

なお、本実施形態においては、送信装置と受信装置の間でやりとりされるAKE
Eコントロールコマンドの転送手順を相互の調停により決定したが、転送手順を
15 決定する手段はこれに限らない。すなわち、複数の転送手順の個々について、あらかじめ定められた優先順位がある場合は、受信装置は、自身が実行可能な手順の中で最も優先順位の高い手順を用いて転送を開始し、送信装置がその手順を実行不能な時には、優先順位にしたがって順次次の手順を選択して転送を開始し、送信装置と受信装置の双方が実行可能な手順が見つかったならば、その手順を用
20 いてAKEコントロールコマンドの転送を行っても、同様の効果が得られることは言うまでもない。

なお、本実施形態においては、送信装置が実データ部の復号に用いる復号化情報を暗号化して、受信装置へ転送したが、受信装置が復号化情報を取得するための手段はこれに限らない。すなわち、送信装置が暗号化した復号化情報を転送す
25 るのではなく、受信装置が復号化情報を取得するのに十分な情報を送信装置が受

信装置に転送し、受信装置がこの情報から間接的に復号化情報を取得してもよい。具体的には、送信装置から受信装置へはハッシュ関数の種だけが転送され、受信装置側では受信した種をもとにハッシュ関数を用いて復号化情報を取得しても同様の効果が得られることは言うまでもない。

- 5 なお、本実施形態においては、AKEコマンドのフォーマットの一例を示したが、AKEコマンドのフォーマットはこれに限らない。すなわち、本実施形態で示したAKEコマンドのフォーマットは、本実施形態を実現するための一例にすぎず、これとは異なるフォーマットのコマンドを用いても同様の効果を得ることができることは言うまでもない。

10

産業上の利用の可能性

- 15 以上のように、本発明のデータ転送方法では、同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データ部と一緒に送信されるデータ転送が行われることにより、同期データを受信した受信装置は、同期データ内に含まれる暗号識別情報を調べ、実データ部が暗号化されていることを検出すると、送信装置に対して実データ部を復号するための復号化情報を要求し、この要求を受けた送信装置は受信装置に対して復号化情報を付与するので、送信装置が受信装置に復号のための鍵情報を付与する際の手順が極めて簡素なデータ転送方法を実現できるとい

- 20 また以上のように本発明のデータ転送方法では、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行ってデータ転送を行うことにより、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が暗号化された同期データを受信しても誤動作する可能性の無いデータ転送方法を実現できるという優れた効果がある。
- 25

また以上のように本発明のデータ転送方法では、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行ってデータ転送を行うことにより、送信装置の送信している同期データを受信装置が継続的に受信している最中に同期データの暗号化が始まったとしても、CIPヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できるという優れた効果がある。

また以上のように本発明のデータ転送方法では、送信装置と受信装置の間でやり取りされる認証情報および復号化情報の授受手順を送信装置と受信装置との間の調停によって選択することにより、将来の拡張性に優れた認証および復号化情報の授受手順を実現することが可能となる。すなわち、将来新しい認証方法や復号化情報が利用可能になった際に、新しい手順を使用できる機器と古い手順しか使用できない機器とが混在しても、新しい機器が古い手順を使用可能であれば、両機器間の調停により最適な手順を選択することが可能になる。すなわち本発明のデータ転送方法では、新しい機器と古い機器とが混在する環境においても、常に最適な手順を選択して実行可能になるという優れた効果がある。

また以上のように本発明のデータ転送方法では、暗号化された実データと暗号化されない実データとの割合を変化させることが可能であるので、暗号化された実データを復号するための高速処理が出来る専用ハードウェアを持たない受信装置でも、ソフトウェアによって復号化が可能になる。すなわち、パソコンのように復号用のハードウェアを持たない機器が受信装置である場合にも、暗号化される実データの割合を低下させ復号化処理を少なくすることにより、処理速度が遅いソフトウェアによる復号が可能になるという優れた効果がある。

また以上のように本発明のデータ転送方法では、送信装置と受信装置が相互に正規の機器であることを認証するまでの間は、実データを含まないアイソクロノ

スパケットを出力するので、限られたバスの転送帯域を無駄に使用することがなく、また正規に認証されていない機器が実データを受信してしまう可能性が非常に少なくなるという優れた効果がある。

請求の範囲

1. バス上の任意の機器が同期データを受信する同期 (isochronousアイソクロノス) 通信と、非同期データを受信する機器が特定される非同期 (asynchronousエイシンクロナス) 通信とが使用されるバスシステムにおいて、
5 前記同期データは実データ部を含む場合があり、前記実データ部の暗号化状況を示す暗号識別情報が前記実データ部以外の前記同期データ中に含まれており、前記同期データを受信した受信装置は、前記実データ部が暗号化されていることを前記暗号識別情報が示している場合には、前記同期データを送信している送信装置
10 に対して、前記非同期通信を用いて前記実データ部の復号化情報を要求し、前記要求を受けた前記送信装置は、前記非同期通信を用いて前記受信装置に対して前記実データ部の前記復号化情報を暗号化した復号化情報、もしくは前記復号化情報を取得するのに必要な復号化情報取得データを送信し、前記受信装置は、前記暗号化された復号化情報を受信した場合には、前記暗号化された復号化情報から
15 前記復号化情報を取り出し、また、前記受信装置が前記復号化情報取得データを受信した場合には、前記復号化情報取得データを用いて前記復号化情報を取得し、このようにして得られた前記復号化情報を用いて暗号化された実データ部を復号することを特徴とするデータ転送方法。

2. 前記同期データを受信した前記受信装置が、前記実データ部が暗号化されていることを検出してから前記復号化情報を取得するまでの一連の手順には、複数の種類が存在し、前記受信装置は、前記復号化情報の要求に先立って、前記送信装置が実行可能な手順の種類を前記送信装置に問い合わせ、前記受信装置は、自身と前記送信装置との双方が前記実行可能な手順の中から実行する手順を選択し、
20 前記受信装置は選択した前記手順に基づいて前記復号化情報を取得すること特徴とする請求項 1 記載のデータ転送方法。
25

3. 前記送信装置と前記受信装置との双方が前記実行可能な手順が複数存在する場合には、あらかじめ定められた優先順位に従って前記手順を選択すること特徴とする請求項2記載のデータ転送方法。

4. 前記同期データを受信した前記受信装置が、前記実データ部が暗号化されていることを検出してから前記復号化情報を取得するまでの前記一連の手順には、複数の種類が存在し、前記受信装置は、前記複数の種類の手順の中からあらかじめ定められた優先順位に従って前記手順を選択して前記手順を開始し、前記受信装置の選択した前記手順を前記送信装置が実行不能である場合には、前記受信装置は、前記送信装置が実行可能な前記手順が見つかるまで、前記手順を順次選択し直して前記手順を開始し、前記受信装置は、実行可能な手順が見つかった時に、その選択した手順に基づいて前記復号化情報を取得すること特徴とする請求項1記載のデータ転送方法。

5. 前記選択された手順に基づいて、前記送信装置と前記受信装置との間で授受される前記非同期データには、実行中の前記手順の種類をあらわす識別子が含まれることを特徴とする請求項2～4のいずれか記載のデータ転送方法。

6. 前記受信装置は、前記復号化情報の要求を行う前に、前記送信装置が正規の送信装置であることを確認することを特徴とする請求項1～5のいずれか記載のデータ転送方法。

7. 前記送信装置は、前記復号化情報の要求を受けた後、受信装置が前記正規の受信装置であることを確認してから、前記実データ部の復号化情報を暗号化して送信することを特徴とする請求項1～5のいずれか記載のデータ転送方法。

8. 前記送信装置と前記受信装置とが、互いに、相手が前記正規の受信装置または前記正規の送信装置であることを確認してから、前記受信装置が前記復号化情報の要求を行うことを特徴とする請求項1～5のいずれか記載のデータ転送方法。

9. 前記受信装置が前記復号化情報を要求する前に、前記受信装置から前記送信

装置に対して、前記送信装置が共通鍵を作成するのに少なくとも必要な情報の送信と、前記送信装置から前記受信装置に対して、前記受信装置が前記共通鍵を作成するのに少なくとも必要な情報の送信とが行われ、前記送信装置は前記共通鍵を用いて前記復号化情報を暗号化して送信し、前記受信装置は受信した前記暗号化された複合化情報から前記共通鍵を用いて前記復号化情報を取り出すことを特徴とする請求項 1 ～ 8 のいずれか記載のデータ転送方法。

10 10. 前記暗号化は前記実データ部に対してのみ行うことを特徴とする請求項 1 ～ 5 のいずれか記載のデータ転送方法。

11. 前記送信装置は内部に実データの信号源を有し、前記送信装置は前記信号源から出力された固定長単位の前記実データ毎に暗号化の有無を決定し、暗号化された前記実データと暗号化されていない前記実データとを互いに異なる前記同期通信の出力単位内に配置して前記バスシステムへ出力することを特徴とする請求項 1 ～ 5 のいずれか記載のデータ転送方法。

12. 前記暗号化された実データと前記暗号化されていない実データとの比率を、前記受信装置が前記送信装置に対して前記非同期通信を用いて指定し、前記送信装置は前記指定に従って暗号化の有無の比率を変更することを特徴とする請求項 11 記載のデータ転送方法。

13. 前記送信装置は内部に前記実データの信号源を有し、前記送信装置は前記信号源から出力された前記固定長単位の実データについて、前記固定長単位の実データ中での前記暗号化を行う割合を決定し、前記実データを前記同期通信の出力単位内に配置して前記バスシステムへ出力することを特徴とする請求項 1 ～ 5 のいずれか記載のデータ転送方法。

14. 前記受信装置は前記送信装置に対して、前記暗号化を行う割合の指定を前記非同期通信によって行い、前記送信装置は前記指定に従って前記暗号化する割合を変更することを特徴とする請求項 13 記載のデータ転送方法。

15. 前記送信装置が前記同期データを送信する際に、少なくとも前記復号化情報を要求されるまでの間は前記同期データに前記実データ部を含めずに送信し、少なくとも前記復号化情報の要求を受け取った後に前記実データ部を含んだ前記同期データの送信を開始することを特徴とする請求項1～5のいずれか記載のデータ転送方法。

5

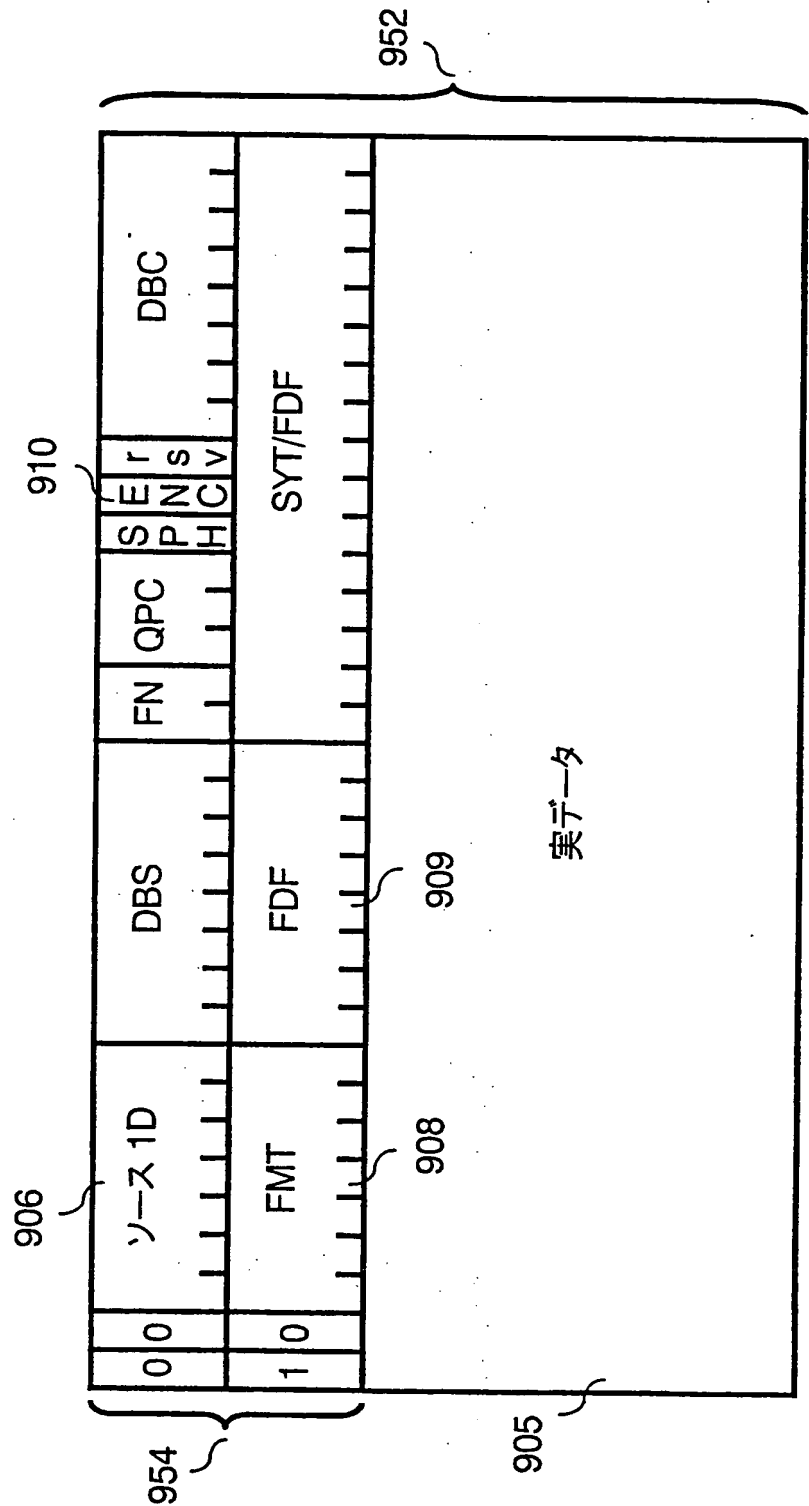


図 1

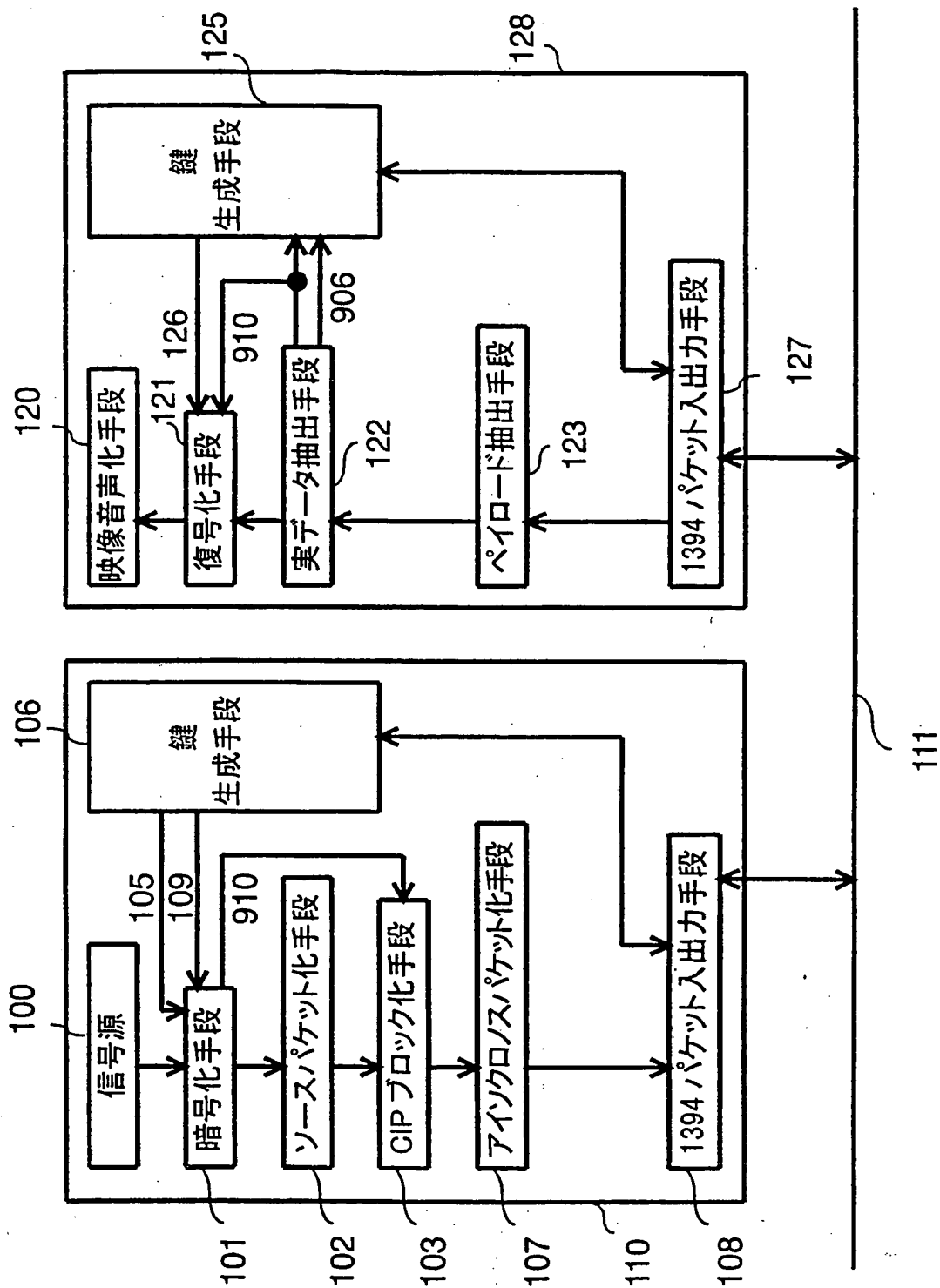


図2

3/7

図 3 A

208 オペコード		msb	lsb
opcode	Authentication and Key exchange		
operand[0]	F ₁₅	アルゴリズム ID	
operand[1]	FF ₁₆		
operand[2]	FF ₁₆		
operand[3]	FF ₁₆		
operand[4]	FF ₁₆		
operand[5]	FF ₁₆		
operand[6]	FF ₁₆		
operand[7]	FF ₁₆		
operand[8]	FF ₁₆		

図 3 B

図 3 B

		208 オペコード						
msb						lsb		
opcode		Authentication and Key exchange						
operand[0]		0		アルゴリズム ID				200
operand[1]		(msb) アルゴリズム領域 (lsb)						201
operand[2]								
operand[3]		FF ₁₆						
operand[4]		FF ₁₆						
operand[5]		FF ₁₆						
operand[6]		FF ₁₆						
operand[7]		(msb) 最大データ長 (lsb)						212
operand[8]								

図 3 C

208 オペコード		msb	lsb
opcode	Authentication and Key exchange		
operand[0]	reserved	アルゴリズム ID	
operand[1]	(msb)	アルゴリズム領域	
operand[2]	(lsb)		
operand[3]	ラベル 202	ステップ番号	
operand[4]	サブファンクション		
operand[5]	チャンネル番号		
operand[6]	ブロック番号 205	総ブロック番号	
operand[7]	(msb)	データ長	
operand[8]	(lsb)		
operand[9]	データ		
operand[8+ data_length]			

4/7

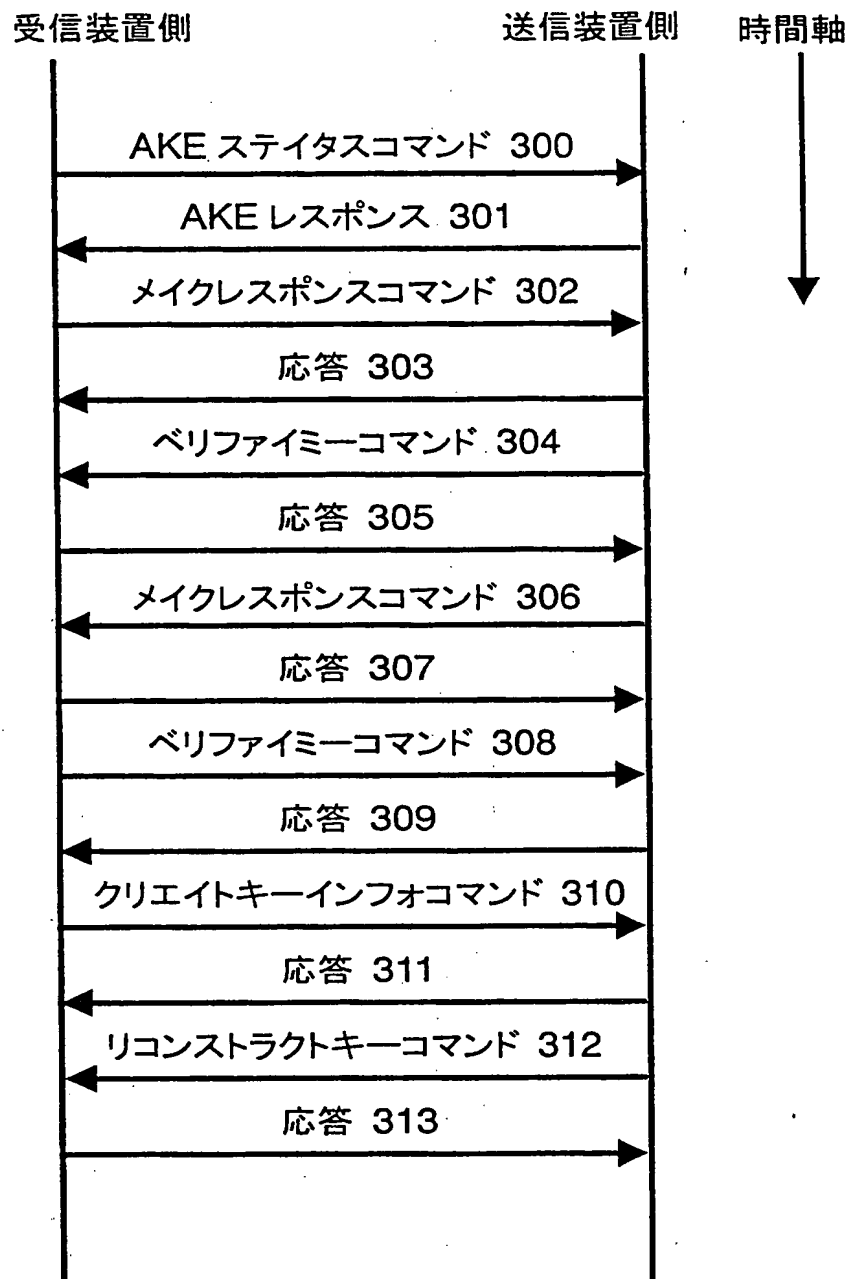


図 4

5/7

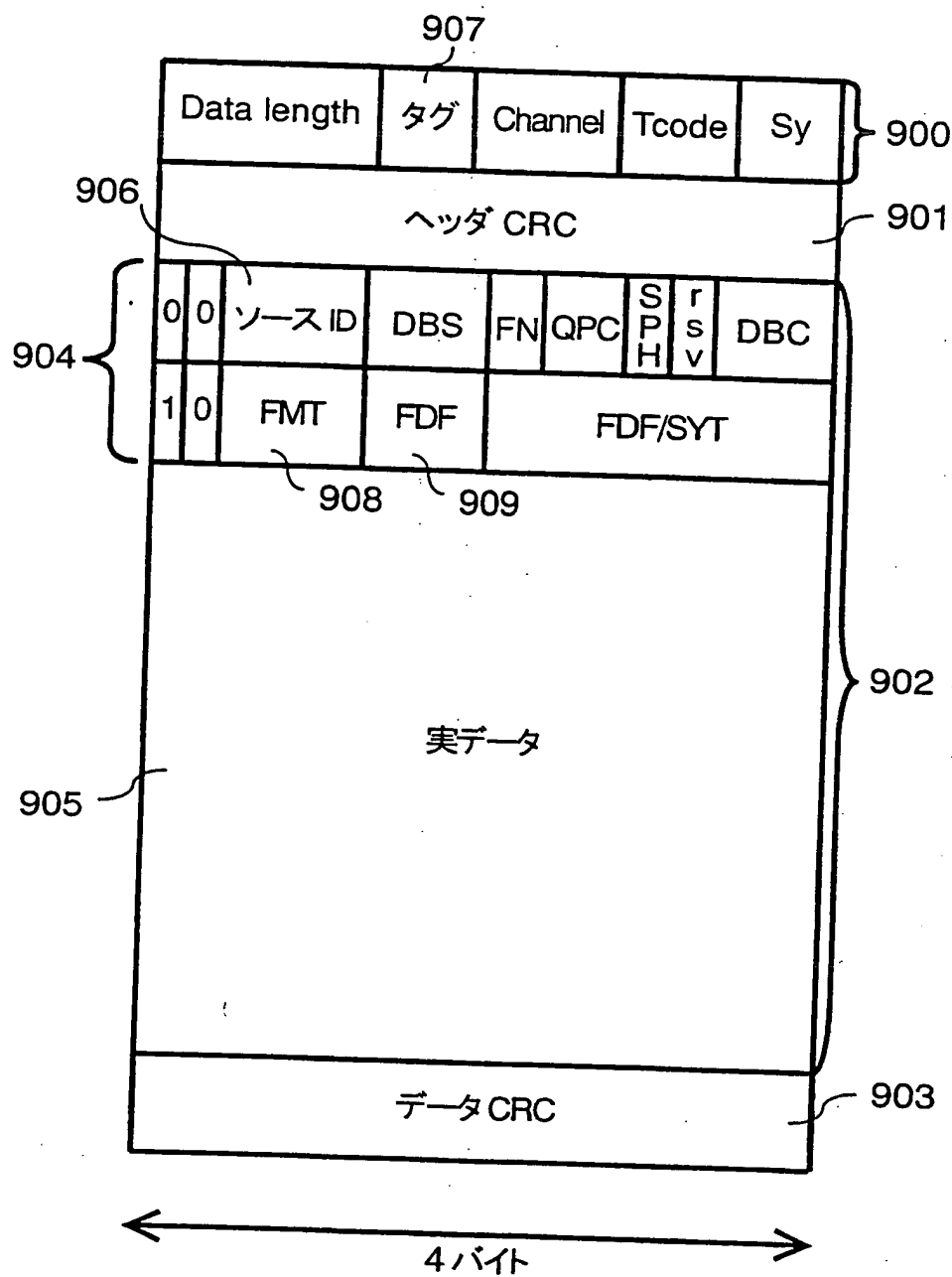


図 5

図面の参照符号の一覧表

100	信号源
101	暗号化手段
102	ソースパケット化手段
103	CIPぶろっく化手段
107	アイソクロノスパケット化手段
108、127	1394パケット入出力手段
105	出力命令
109、126	暗号鍵
110	送信装置
128	受信装置
111	IEEE1394バス
106、125	鍵生成手段
120	映像音声化手段
121	複合化手段
122	実データ抽出手段
123	ペイロード抽出手段
200	アルゴリズムID
201	アルゴリズム領域
202	ラベル
203	ステップ番号
204	チャンネル番号
205	ブロック番号
206	総ブロック数
207	データ
208	オペコード
209	データ長

- 212 最大データ長
- 299 サブファンクション
- 300 AKEステイタスコマンド
- 301 AKEレスポンス
- 302、306 メイクレスポンスコマンド
- 303、305、307、309、311、313 応答
- 304、308 ベリファイミーコマンド
- 310 クリエイトキーインフォコマンド
- 312 リコンストラクトキーコマンド
- 900 アイソクロノスケットヘッダ
- 901 ヘッダCRC
- 902、952 アイソクロノスペイロード
- 903 データCRC
- 904、954 CIPヘッダ
- 905 実データ
- 906 ソースID
- 907 タグ
- 908 FMT
- 909 FDF
- 910 暗号化情報 (ENC)
- 952 アイソクロノスペイロード

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP98/01837

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁶ H04L12/40, H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁶ H04L12/28, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1998 Toroku Jitsuyo Shinan Koho 1994-1998
Kokai Jitsuyo Shinan Koho 1971-1998 Jitsuyo Shinan Toroku Koho 1996-1998

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 61-260735, A (Fujitsu Ltd.), November 18, 1986 (18. 11. 86) (Family: none)	1-15
A	JP, 61-81043, A (Fujitsu Ltd.), April 24, 1986 (24. 04. 86) (Family: none)	1-15
A	JP, 01-307341, A (Fujitsu Ltd.), December 12, 1989 (12. 12. 89) (Family: none)	1-15
A	JP, 01-181349, A (Nippon Telegraph & Telephone Corp.), July 19, 1989 (19. 07. 89) (Family: none)	1-15
A	JP, 09-205421, A (Canon Inc.), August 5, 1997 (05. 08. 97) (Family: none)	1-15

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
July 13, 1998 (13. 07. 98)

Date of mailing of the international search report
July 28, 1998 (28. 07. 98)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

国際調査報告

国際出願番号 PCT/JP98/01837

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl^o H04L12/40
Int. Cl^o H04L9/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl^o H04L12/28
Int. Cl^o H04L9/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1998年
日本国公開実用新案公報 1971-1998年
日本国登録実用新案公報 1994-1998年
日本国実用新案登録公報 1996-1998年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 61-260735, A (富士通株式会社) 18. 11月. 1986 (18. 11. 86) (ファミリーなし)	1-15
A	JP, 61-81043, A (富士通株式会社) 24. 4月. 1986 (24. 04. 86) (ファミリーなし)	1-15
A	JP, 01-307341, A (富士通株式会社) 12. 12月. 1989 (12. 12. 89) (ファミリーなし)	1-15
A	JP, 01-181349, A (日本電信電話株式会社) 19. 7月. 1989 (19. 07. 89) (ファミリーなし)	1-15

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」先行文献ではあるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

13. 07. 98

国際調査報告の発送日

28.07.98

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

矢頭 尚之

5K

8838

電話番号 03-3581-1101 内線 3556

様式PCT/ISA/210 (第2ページ) (1992年7月)

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 09-205421, A (キャノン株式会社) 5. 8月. 1997 (05. 08. 97) (ファミリーなし)	1 - 15

This Page Blank (uspto)